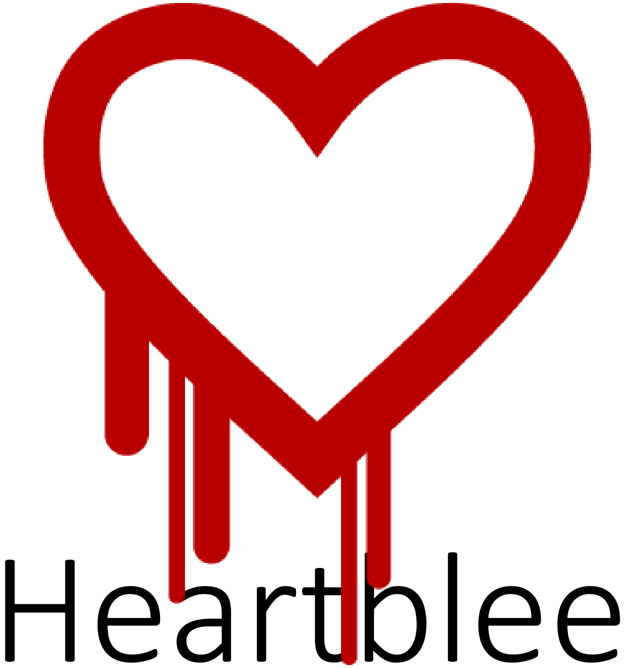


The Heartbleed Bug

Justin Williams

Risk Security Governance & Compliance

Enterprise Information Management Services

TRANSNET

delivering freight reliably

Areas of interest

- Introduction
- How it works
- What is affected
- What to do
- Checking
- Discussion

Introduction

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Source Heartbleed.com

Video

- In this SOC Talk, Elastica's CTO Dr. Zulfikar Ramzan walks through the mechanics of the Heartbeatbleed bug

- **http://vimeo**.com/91425662

What is affected?

- Servers
  - HTTPS
  - FTPS
  - SSL VPN
  - Secure SMTP/POP/IMAP
  - Virtualisation platform (VMWare)
  - Any service secured by SSL
- Devices
  - Lots

What do we (admins) need to do?

- Check for vulnerability (Vendor + Scanning)
- Patch
  - 20% of vulnerable servers on 7th May were not vulnerable on 11 April (The Register)
  - 318 239 of 600 000 still vulnerable on 7th May
- Replace certificates
  - 66% of certificates on previously vulnerable servers “soiled”
  - Some CA’s automatically de-activate old (GoDaddy)
  - “The main concern is that mass revocation of SSL certificates will cause strain on CA infrastructure.”

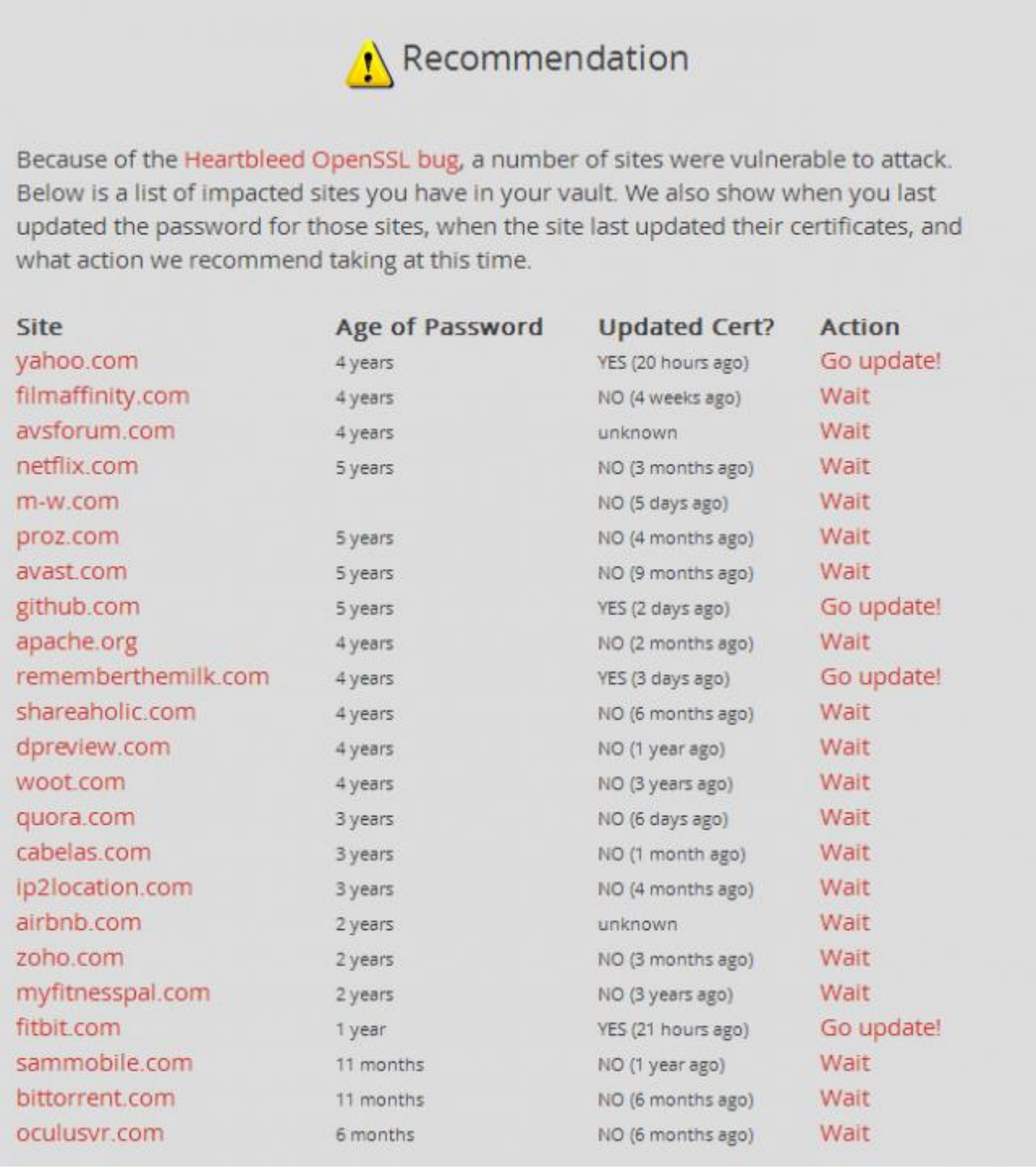
What do we (users) need to do?

- Check your devices (especially internet facing)
  - Routers, cloud devices, ADSL modems
- Consider changing passwords
  - 630 of top 10 000 sites vulnerable on 8 April 2014
  - Including :
    - Yahoo, Imgur, Flickr
    - Eventbrite, mail.com, indiegogo
    - Lonelyplanet, Kaspersky, Rapidshare
    - Creativecommons.org, bidorbuy.co.za
    - DigitalRiver, Barclaycardus, utorrent.com

What do we (users) need to do?

- Consider LastPass

- Manages your passwords
- Quickly built a tool to check Heartbleed across all your managed accounts



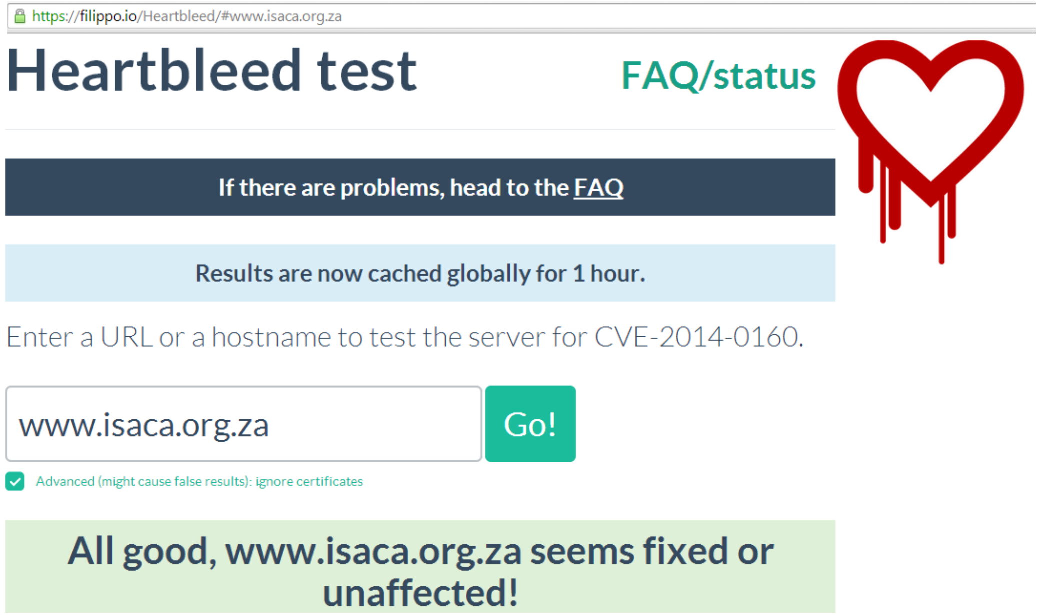
⚠ Recommendation

Because of the Heartbleed OpenSSL bug, a number of sites were vulnerable to attack. Below is a list of impacted sites you have in your vault. We also show when you last updated the password for those sites, when the site last updated their certificates, and what action we recommend taking at this time.

Site	Age of Password	Updated Cert?	Action
yahoo.com	4 years	YES (20 hours ago)	Go update!
filmaffinity.com	4 years	NO (4 weeks ago)	Wait
avsforum.com	4 years	unknown	Wait
netflix.com	5 years	NO (3 months ago)	Wait
m-w.com		NO (5 days ago)	Wait
proz.com	5 years	NO (4 months ago)	Wait
avast.com	5 years	NO (9 months ago)	Wait
github.com	5 years	YES (2 days ago)	Go update!
apache.org	4 years	NO (2 months ago)	Wait
rememberthemilk.com	4 years	YES (3 days ago)	Go update!
shareaholic.com	4 years	NO (6 months ago)	Wait
dpreview.com	4 years	NO (1 year ago)	Wait
woot.com	4 years	NO (3 years ago)	Wait
quora.com	3 years	NO (6 days ago)	Wait
cabelas.com	3 years	NO (1 month ago)	Wait
ip2location.com	3 years	NO (4 months ago)	Wait
airbnb.com	2 years	unknown	Wait
zoho.com	2 years	NO (3 months ago)	Wait
myfitnesspal.com	2 years	NO (3 years ago)	Wait
fitbit.com	1 year	YES (21 hours ago)	Go update!
sammobile.com	11 months	NO (1 year ago)	Wait
bittorrent.com	11 months	NO (6 months ago)	Wait
oculusvr.com	6 months	NO (6 months ago)	Wait

Checking for vulnerability

- Websites
  - ***https://filippo.io/Heartbleed***
- ***Tools***
  - ***Nmap (grab banners)***
  - ***CrowdStrike Heartbleed Scanner***



https://filippo.io/Heartbleed/#www.isaca.org.za

Heartbleed test

FAQ/status

If there are problems, head to the FAQ

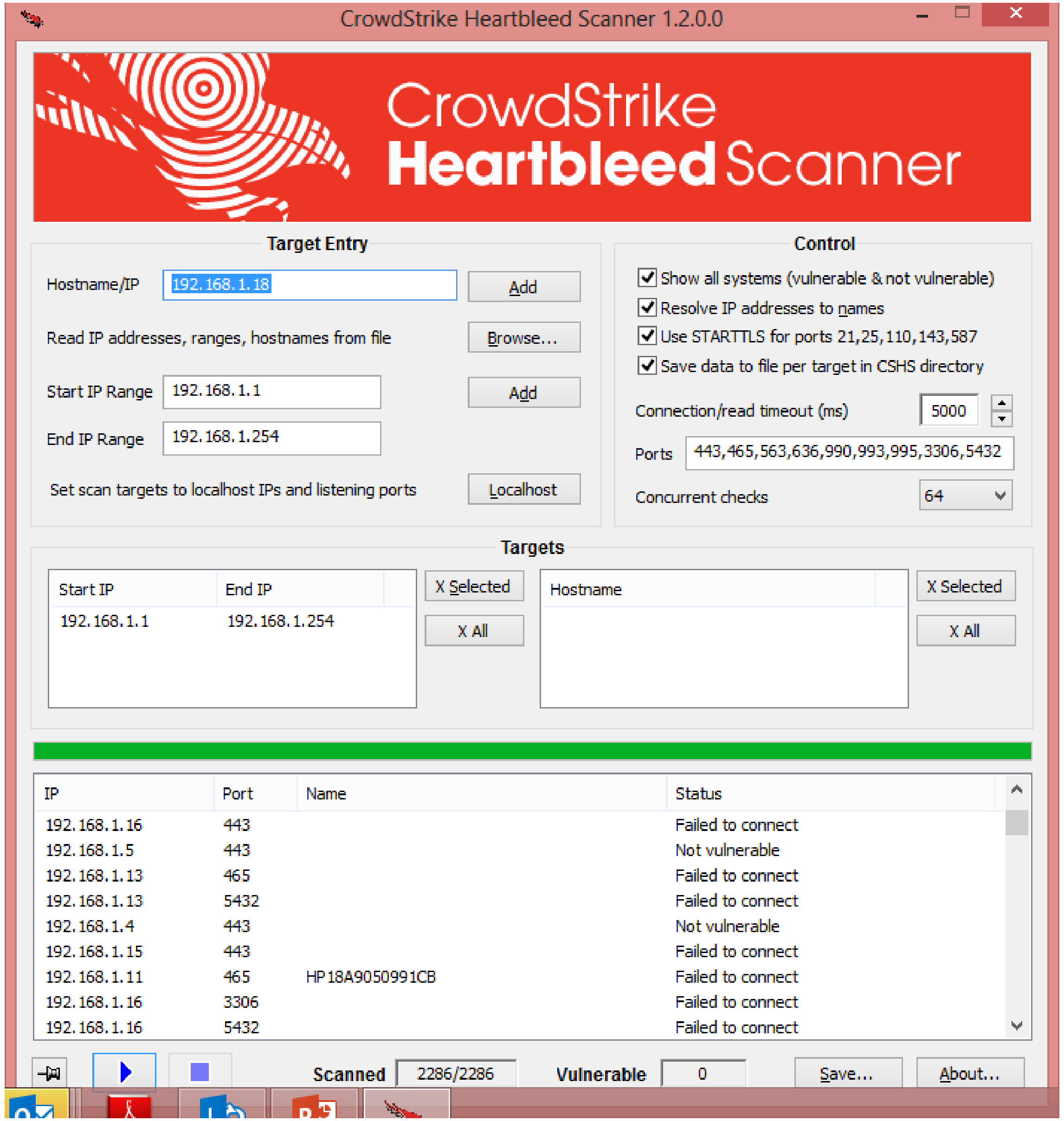
Results are now cached globally for 1 hour.

Enter a URL or a hostname to test the server for CVE-2014-0160.

www.isaca.org.za

☑ Advanced (might cause false results): ignore certificates

All good, www.isaca.org.za seems fixed or unaffected!



CrowdStrike Heartbleed Scanner 1.2.0.0

CrowdStrike **Heartbleed** Scanner

Target Entry

Hostname/IP: 192.168.1.18

Read IP addresses, ranges, hostnames from file

Start IP Range: 192.168.1.1

End IP Range: 192.168.1.254

Set scan targets to localhost IPs and listening ports

Control

- ☑ Show all systems (vulnerable & not vulnerable)
- ☑ Resolve IP addresses to names
- ☑ Use STARTTLS for ports 21,25,110,143,587
- ☑ Save data to file per target in CSHS directory

Connection/read timeout (ms): 5000

Ports: 443,465,563,636,990,993,995,3306,5432

Concurrent checks: 64

Targets

Start IP	End IP
192.168.1.1	192.168.1.254

IP	Port	Name	Status
192.168.1.16	443		Failed to connect
192.168.1.5	443		Not vulnerable
192.168.1.13	465		Failed to connect
192.168.1.13	5432		Failed to connect
192.168.1.4	443		Not vulnerable
192.168.1.15	443		Failed to connect
192.168.1.11	465	HP18A9050991CB	Failed to connect
192.168.1.16	3306		Failed to connect
192.168.1.16	5432		Failed to connect

Scanned: 2286/2286 Vulnerable: 0

http://www.crowdstrike.com/community-tools/index.html

TRANSNET
delivering freight reliably

That’s me, I’m done ;)

- Discussion / Questions

- Contact
  - Justin.Williams@transnet.net
  - Justin.j.Williams@gmail.com
  - @jjza
  - j-j.co.za